HashiCorp

Exam Questions HCVA0-003

HashiCorp Certified: Vault Associate (003)Exam

NEW QUESTION 1
- (Topic 1)
When using the Vault Secrets Operator, where is the secret written to after being retrieved from Vault?

A. The secret is never written to any service or persistent storage
B. Directly to the filesystem of the pod
C. Kubernetes Secrets
D. To the cloud-provider??s native secret manager (Azure Key Vault, AWS Secrets Manager, etc.)

Answer: C

NEW QUESTION 2
- (Topic 1)
From the unseal options listed below, select the options you can use if you're deploying Vault on-premises (select four).

A. Certificates
B. Transit
C. AWS KMS
D. HSM PKCS11
E. Key shards

Answer: BCDE

NEW QUESTION 3
- (Topic 1)
According to the screenshot below, what auth method did this client use to log in to Vault? (Screenshot shows a lease path: auth/userpass/login/student01)

A. Userpass
B. Auth
C. Root token
D. Child token

Answer: A

NEW QUESTION 4
- (Topic 1)
What is the difference between the TTL and the Max TTL (select two)?

A. The TTL defines when the token will expire and be revoked
B. The TTL defines when another token will be generated
C. The Max TTL defines the timeframe for which a token cannot be used
D. The Max TTL defines the maximum timeframe for which a token can be renewed

Answer: AD

NEW QUESTION 5
- (Topic 1)
True or False? The Vault Secrets Operator does NOT encrypt client cache, such as Vault tokens and leases, by default in Kubernetes Secrets.

A. True
B. False

Answer: A

NEW QUESTION 6
- (Topic 1)
In regards to the Transit secrets engine, which of the following is true given the following command and output (select three):
$ vault write encryption/encrypt/creditcard plaintext=$(base64 <<< "1234 5678 9101 1121") Key: ciphertext Value: vault:v3:cZNHVx+sxdMErXRSuDa1q/pz49fXTn1PScKfhf+PIZPvy8xKfkytpwKcbC0fF2U=

A. The Transit secrets engine is mounted at the encryption path
B. The name of the keyring used to encrypt the data is creditcard
C. There are at least three data keys associated with this keyring
D. The data was written to the encryption path, which is provided by default when enabling the Transit secrets engine

Answer: ABC

NEW QUESTION 7
- (Topic 1)
How can Vault be used to programmatically obtain a generated code for MFA, somewhat similar to Google Authenticator?

A. Cubbyhole
B. The random byte generator
C. TOTP secrets engine
D. The identity secrets engine

Answer: C

NEW QUESTION 8
- (Topic 1)
When generating dynamic credentials, Vault also creates associated metadata, including information like time duration, renewability, and more, and links it to the credentials. What is this referred to as?

A. Secret
B. Token
C. Lease
D. Secrets engine

Answer: C

NEW QUESTION 9
- (Topic 1)
You want to integrate a third-party application to retrieve credentials from the HashiCorp Vault API. How can you accomplish this without having direct access to the source code?

A. You cannot integrate a third-party application with Vault without being able to modify the source code
B. Put in a request to the third-party application vendor
C. Instead of the API, have the application use the Vault CLI to retrieve credentials
D. Use the Vault Agent to obtain secrets and provide them to the application

Answer: D

NEW QUESTION 10
- (Topic 1)
Jason has enabled the userpass auth method at the path users/. What path would Jason and other Vault operators use to interact with this new auth method?

A. users/auth/
B. authentication/users
C. auth/users
D. users/

Answer: C

NEW QUESTION 10
- (Topic 1)
What is true about the output of the following command (select three)?

A. The admin never sees all the unseal keys and cannot unseal Vault by themselves
B. All three users, Jane/John/Student01, will receive all unseal keys and can unseal Vault
C. The admin will receive the unseal keys and be able to unseal Vault themselves
D. The keys will be returned encrypted
E. Each individual can only decrypt their own unseal key using their private PGP key

Answer: ADE

NEW QUESTION 15
- (Topic 1)
You??ve set up multiple Vault clusters, one on-premises intended to be the primary cluster, and the second cluster in AWS, which was deployed for performance replication. After enabling replication, developers complain that all the data they??ve stored in the AWS Vault cluster is missing. What happened?

A. There is a certificate mismatch after replication was enabled since Vault replication generates its own TLS certificates to ensure nodes are trusted entities
B. All of the data on the secondary cluster was deleted after replication was enabled
C. The data was automatically copied to the primary cluster after replication was enabled since all writes are always forwarded to the primary cluster
D. The data was moved to a recovery path after replication was enable
E. Use the vault secrets move command to move the data back to its intended location

Answer: B

NEW QUESTION 18
- (Topic 1)
Which of the following policies would permit a user to generate dynamic credentials on a database?

A. path "database/creds/read_only_role" { capabilities = ["generate"] }
B. path "database/creds/read_only_role" { capabilities = ["update"] }
C. path "database/creds/read_only_role" { capabilities = ["list"] }
D. path "database/creds/read_only_role" { capabilities = ["read"] }

Answer: D

NEW QUESTION 21
- (Topic 1)

What are the primary benefits of running Vault in a production deployment over dev server mode (select two)?

A. Faster deployment
B. Persistent storage
C. Ability to enable auth methods
D. Encryption via TLS

Answer: BD

NEW QUESTION 23
- (Topic 1)
From the options below, select the benefits of using a batch token over a service token (select four).

A. Often used for ephemeral, high-performance workloads
B. Can be a root token
C. Can be used on performance replication clusters (if orphan)
D. Has accessors
E. Lightweight and scalable
F. No storage cost for token creation

Answer: ACEF

NEW QUESTION 26
- (Topic 1)
When configuring Vault replication and monitoring its status, you keep seeing something called 'WALs'. What are WALs?

A. Warning of allocated logs
B. Write along logging
C. Write-ahead logs
D. Wake after LAN

Answer: C

NEW QUESTION 27
- (Topic 1)
You logged into the Vault CLI and attempted to enable an auth method, but you received this error message. What can you do to resolve the error and configure Vault?
(Error: dial tcp 127.0.0.1:8200: connect: connection refused)

```
bk~$vault secrets enable transit
Error enabling: Post "https://127.0.0.1:8200/v1/sys/mounts/transit": http: server
 gave HTTP response to HTTPS client
bk~$
```

A. Restart the Vault service on this node
B. Ask an admin to grant you permission to enable the userpass auth method
C. Change 'userpass' to 'username and password'
D. Set the VAULT_ADDR environment variable to HTTP

Answer: D

NEW QUESTION 30
- (Topic 1)
Select the policies below that permit you to create a new entry of environment=prod at the path /secrets/apps/my_secret (select three).

A. path "secrets/+/my_secret" { capabilities = ["create"] allowed_parameters = { "*" = [] } }
B. path "secrets/apps/my_secret" { capabilities = ["update"] }
C. path "secrets/apps/my_secret" { capabilities = ["create"] allowed_parameters = { "environment" = [] } }
D. path "secrets/apps/*" { capabilities = ["create"] allowed_parameters = { "environment" = ["dev", "test", "qa", "prod"] } }

Answer: ACD

NEW QUESTION 32
- (Topic 1)
From the options below, select the benefits of using the PKI (x.509 certificates) secrets engine (select three):

A. TTLs on Vault certs are longer to ensure certificates are valid for a longer period of time
B. Reducing, or eliminating certificate revocations
C. Reduces time to get a certificate by eliminating the need to generate a private key and CSR
D. Vault can act as an intermediate CA

Answer: BCD

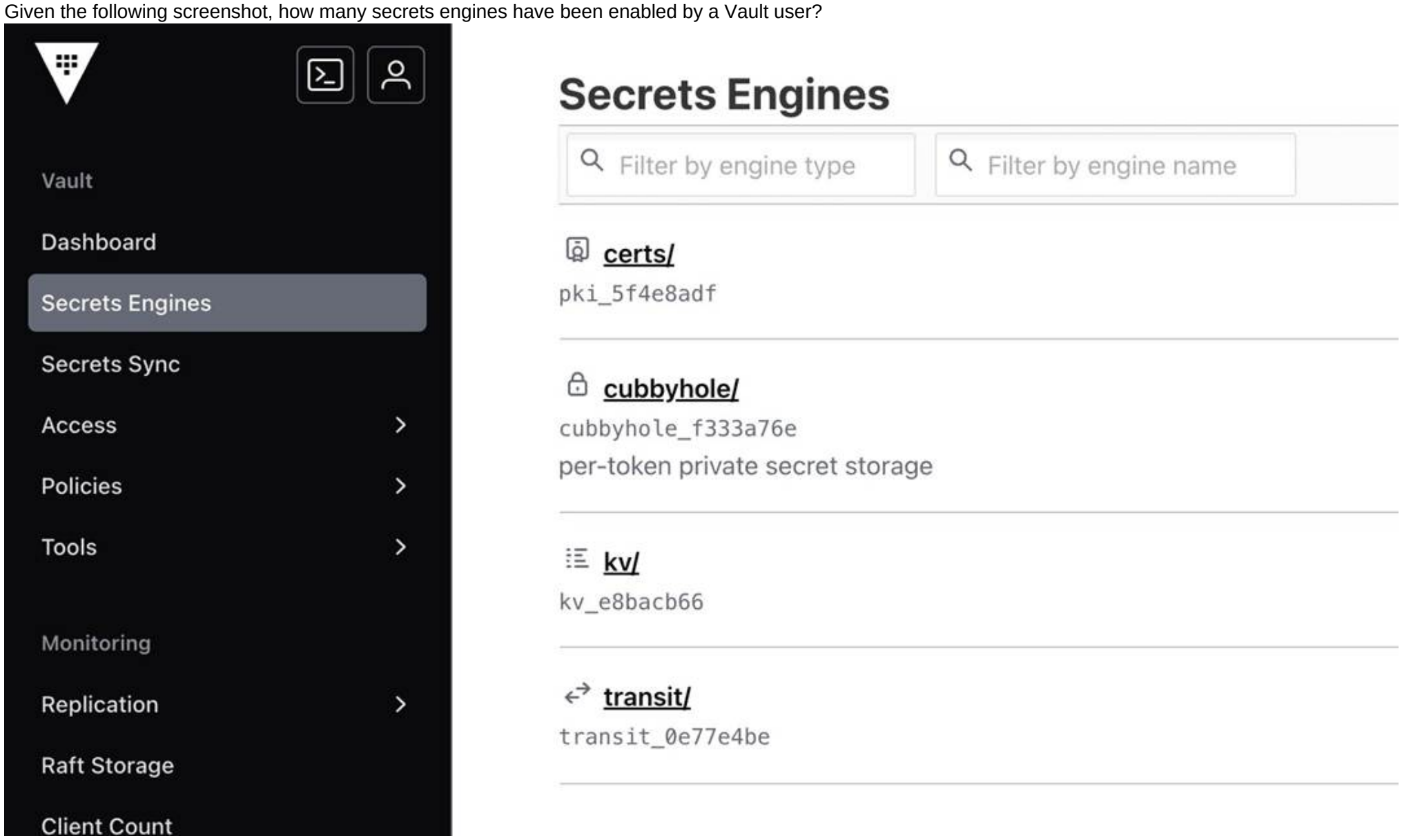
NEW QUESTION 34

- (Topic 1)
Given the following policy, which command below would not result in a permission denied error (select two)?
path "secret/*" { capabilities = ["create", "update"] allowed_parameters = { "student" = ["steve", "frank", "jamie", "susan", "gerry", "damien"] } }
path "secret/apps/*" { capabilities = ["read"] }
path "secret/apps/results" { capabilities = ["deny"] }

A. vault kv put secret/apps/results student03=practice
B. vault kv put secret/apps/app01 student=bryan
C. vault kv put secret/common/results student=frank
D. vault kv get secret/apps/api_key

Answer: CD

NEW QUESTION 39
- (Topic 1)
Given the following screenshot, how many secrets engines have been enabled by a Vault user?



A. 2
B. 3
C. 4
D. 5

Answer: B

NEW QUESTION 43
- (Topic 1)
After encrypting data using the Transit secrets engine, you??ve received the following output. Which of the following is true based on the output displayed below?
Key: ciphertext Value: vault:v2:45f9zW6cglbrzCjl0yCyC6DBYtSBSxnMgUn9B5aHcGEit71xefPEmmjMbrk3

A. The original encryption key has been rotated at least once
B. The data is stored in Vault using a KV v2 secrets engine
C. This is the second version of the encrypted data
D. Similar to the KV secrets engine, the Transit secrets engine was enabled using the transit v2 option

Answer: A

NEW QUESTION 48
- (Topic 1)
Which of the following Vault policies will allow a Vault client to read a secret stored at secrets/applications/app01/api_key?

A. path "secrets/applications/" { capabilities = ["read"] allowed_parameters = { "certificate" = [] } }
B. path "secrets/*" { capabilities = ["list"] }
C. path "secrets/applications/+/api_*" { capabilities = ["read"] }
D. path "secrets/applications/app01/api_key/*" { capabilities = ["update", "list", "read"] }

Answer: C

NEW QUESTION 49
- (Topic 1)
True or False? All dynamic secrets in Vault are required to have a lease.

A. True
B. False

Answer: A

NEW QUESTION 50
- (Topic 1)
After decrypting data using the Transit secrets engine, the plaintext output does not match the plaintext credit card number that you encrypted. Which of the following answers provides a solution?
$ vault write transit/decrypt/creditcard ciphertext="vault:v1:cZNHVx+sxdMEr....." Key: plaintext Value: Y3JlZGl0LWNhcmQtbnVtYmVyCg==

A. Vault is sealed, therefore the data cannot be decrypte
B. Unseal Vault to properly decrypt the data
C. The user doesn??t have permission to decrypt the data, therefore Vault returns false data
D. The resulting plaintext data is base64-encode
E. To reveal the original plaintext, use the base64 --decode command
F. The data is corrupte
G. Execute the encryption command again using a different data key

Answer: C

NEW QUESTION 51
- (Topic 1)
After issuing the command to delete a secret, you run a vault kv list command, but the path to the secret still seems to exist. What command would permanently delete the path from Vault?

```
$ vault kv delete kv/applications/app01
Success! Data deleted (if it existed) at: kv/applications/app01
$ vault kv list kv/applications
Keys
----
app01
```

A. vault kv delete -force kv/applications/app01
B. vault kv destroy -versions=1 kv/applications/app01
C. vault kv metadata delete kv/applications/app01
D. vault kv delete -all kv/applications/app01

Answer: C

NEW QUESTION 53
- (Topic 2)
Christy has created a token and needs to use that token to access Vault. What command can she use to authenticate and access secrets stored in Vault?
$ vault token create -policy=christy Key Value
--- -----
token hvs.hxDIPd8RPVtxu4AzSGS1lArP token_accessor AxwxpDs6LbdFQbWGmBDnwIK3 token_duration 24h
token_renewable true token_policies ["christy" "default"] identity_policies []
policies ["christy" "default"]

A. vault login hvs.hxDIPd8RPVtxu4AzSGS1lArP
B. vault login -method=password
C. vault login -method=token christy
D. vault login -accessor=AxwxpDs6LbdFQbWGmBDnwIK3

Answer: A

NEW QUESTION 54
- (Topic 2)
Which of the following statements best describes the difference between static and dynamic credentials in a secrets management system?

A. They are functionally identical—the only difference is what secrets engine creates them.
B. Static credentials only apply to specific use cases, while dynamic credentials can be used everywhere.
C. Static credentials often remain persistent for long periods of time, while dynamic are short-lived and auto-rotated.
D. Static credentials are ephemeral and rotated frequently, while dynamic credentials remain unchanged indefinitely.

Answer: C

NEW QUESTION 58
- (Topic 2)
Which of the following best describes a token accessor?

A. A value that describes which clients have access to the attached token
B. Describes the value associated with the token??s TTL
C. A token used for clients to access Vault secrets engines
D. A value that acts as a reference to a token which can be used to perform limited actions against the token

Answer: D

NEW QUESTION 59
- (Topic 2)
The Vault Agent provides which of the following benefits? (Select three)

A. Token renewal
B. Authentication to Vault
C. Client-side caching of responses
D. Automatically creates secrets in the desired storage backend

Answer: ABC

NEW QUESTION 60
- (Topic 2)
After a client has authenticated to Vault, what security feature is used to make all subsequent calls?

A. ldap
B. pgp
C. path
D. key shard
E. listener
F. token

Answer: F

NEW QUESTION 65
- (Topic 2)
After creating a dynamic credential on a database, the DBA accidentally deletes the credentials on the database itself. When attempting to remove the lease, Vault returns an error stating that the credential cannot be found. What command can be run to make Vault remove the secret?

A. vault lease revoke -force -prefix <lease_path>
B. vault lease -renew
C. vault lease revoke -enforce
D. vault revoke -apply

Answer: A

NEW QUESTION 67
- (Topic 2)
True or False? All Vault policies are deny by default.

A. True
B. False

Answer: A

NEW QUESTION 70
- (Topic 2)
What command is used to extend the TTL of a token, if permitted?

A. vault token revoke <token-id>
B. vault capabilities <token-id>
C. vault token lookup <token-id>
D. vault token renew <token-id>

Answer: D

NEW QUESTION 73
- (Topic 2)
You are using Azure Key Vault for the auto-unseal configuration on your cluster. After the Vault service restarts, what command must you run to unseal Vault?

A. You don??t need to run a command when using auto-unseal
B. vault operator members
C. vault operator unseal
D. vault operator init

Answer:

A

NEW QUESTION 76
- (Topic 2)
By default, what happens to child tokens when a parent token is revoked?

A. The child tokens are revoked
B. The child tokens are renewed
C. The child tokens are converted to parent tokens
D. The child tokens create their own child tokens to be used

Answer: A

NEW QUESTION 79
- (Topic 2)
Which of the following best describes the function of the Vault Secrets Operator in a Kubernetes environment?

A. It replaces the Kubernetes secrets API entirely and operates purely as a certificate authority for all workloads.
B. It is a standalone Vault server that automatically applies security policies and rotates root tokens.
C. It continuously reconciles and synchronizes secrets from Vault to Kubernetes, ensuring secrets are always updated
D. It provides an interface to dynamically provision Kubernetes clusters through Vault??s infrastructure secrets.

Answer: C

NEW QUESTION 80
- (Topic 2)
When Vault is sealed, which are the only two operations available to a Vault administrator? (Select two)

A. View the status of Vault
B. Configure policies
C. View data stored in the key/value store
D. Rotate the encryption key
E. Unseal Vault
F. Author security policies

Answer: AE

NEW QUESTION 85
- (Topic 2)
Compared to service tokens, batch tokens are ideal for what type of action?

A. Generating dynamic credentials
B. Renewing other tokens
C. For daily batch jobs requesting secrets from Vault
D. Short-lived, high-volume, or ??ephemeral?? tasks

Answer: D

NEW QUESTION 87
- (Topic 2)
Which auth method is ideal for machine-to-machine authentication?

A. Okta
B. UserPass
C. GitHub
D. AppRole

Answer: D

NEW QUESTION 88
- (Topic 2)
You have a legacy application that requires secrets from Vault that must be written to a local configuration file. However, you cannot refactor the application to communicate directly with Vault.What solution should you implement to satisfy the requirements?

A. Run the Vault Agent and use the templating feature
B. Use the Vault Proxy with Auto-Auth to authenticate with Vault
C. Use the Vault Proxy to act as a proxy for the Vault API
D. Use the Vault Agent and cache the newly created tokens and leases

Answer: A

NEW QUESTION 91
- (Topic 2)
What is the correct order that Vault uses to protect data?

A. root key --> encryption key --> data

B. unseal keys --> root key --> data
C. root key --> data
D. encryption key --> root key --> data

Answer: A

NEW QUESTION 95
- (Topic 2)
Which isnota capability that can be used when writing a Vault policy?

A. delete
B. modify
C. create
D. list
E. read
F. update

Answer: B

NEW QUESTION 98
- (Topic 2)
You have deployed an application that needs to encrypt data before writing to a database. What secrets engine should you use?

A. Transit
B. SSH
C. PKI
D. TOTP

Answer: A

NEW QUESTION 102
- (Topic 2)
True or False? After initializing Vault or restarting the Vault service, each individual node in the cluster needs to be unsealed.

A. True
B. False

Answer: A

NEW QUESTION 105
- (Topic 2)
Your organization wants to set up human-based authentication for AzureAD. What authentication method should you enable and configure for Vault?

A. OIDC/JWT
B. Okta
C. Active Directory
D. UserPass

Answer: A

NEW QUESTION 106
- (Topic 2)
Which of the following unseal options can automatically unseal Vault upon the start of the Vault service? (Select four)

A. HSM
B. Azure KMS
C. AWS KMS
D. Transit
E. Key Shards

Answer: ABCD

NEW QUESTION 107
- (Topic 2)
Which statement most accurately describes how the response wrapping feature functions in Vault?

A. Vault takes the response it would have sent to an HTTP client and instead inserts it into the cubbyhole of a single-use token, returning that single-use token instead.
B. Vault encrypts the response with a dedicated key and sends it directly to the client, never storing it on the server or using single-use tokens for additional security.
C. Vault divides the response into separate parts and stores each part in different tokens, requiring all tokens to be combined before disclosing the secret to the requesting client.
D. Vault duplicates the response within a persistent token and allows multiple unwraps, ensuring that any user with the correct token can retrieve the secret repeatedly without time restrictions.

Answer: A

NEW QUESTION 109
- (Topic 2)
Which of the following are benefits of using the Vault Secrets Operator (VSO)? (Select three)

A. Support for syncing from multiple secret sources
B. Bi-directional sync between Vault and Kubernetes Secrets
C. Automatic secret drift and remediation
D. Automatic secret rotation for multiple Kubernetes resource types

Answer: ACD

NEW QUESTION 113
- (Topic 2)
You have a long-running app that cannot handle a regeneration of a token or secret. What type of token should be created for this application in order to authenticate and interact with Vault?

A. Service Token with Use Limit
B. Periodic Service Token
C. Batch Token
D. Orphan Token

Answer: B

NEW QUESTION 117
- (Topic 2)
You are trying to create a new orphan token but receiving a Permission Denied error. What capabilities are required to create this token without using a root token?

A. write privileges on the path auth/token
B. write privileges on the path sys/mounts
C. sudo privileges on the path auth/token/create
D. sudo privileges on the path sys/mounts/token

Answer: C

NEW QUESTION 121
- (Topic 2)
Holly has discovered that a highly privileged dynamic credential with a very long lease time was created, which could negatively impact the organization??s security. What command can Holly use to invalidate the credential so it can??t be used without affecting other credentials?

A. vault lease revoke aws/creds/admin/27e1b9a1-27b8-83d9-9fe0-d99d786bdc83
B. Holly would need to delete the credential on the cloud platform directly
C. vault lease revoke -all
D. vault lease revoke aws/creds/admin/*

Answer: A

NEW QUESTION 124
- (Topic 3)
Your organization operates active/active applications across multiple data centers for high availability. Which Vault feature should be used in the secondary data centers to provide local access to secrets?

A. Performance standby nodes
B. Customized plugins for the Vault cluster
C. Disaster recovery cluster
D. Performance replication cluster

Answer: D

NEW QUESTION 129
- (Topic 3)
Kyle enabled the database secrets engine for dynamic credentials. Amy, the senior DBA, accidentally deleted the database users created by Vault, disrupting client applications.
How can Kyle manually remove the leases in Vault?

A. No action is required since the leases will eventually expire and be revoked
B. Obtain the individual lease IDs from the application logs and remove them using the vault lease revoke command
C. Use the command vault lease revoke -force flag to delete the leases
D. Revoke all of the leases associated with the entire database secrets engine to be sure they are all removed

Answer: C

NEW QUESTION 132
- (Topic 3)
You have ciphertext stored in an Amazon S3 bucket encrypted by the key named prod- customer. Will Vault decrypt this data with the command vault write transit/decrypt/prod- customer ciphertext="vault:v4:Xa1f9FlJtn13em/Wb7QCsXsU/kCOn7..." given this output?
? $ vault read transit/keys/prod-customer
? Key Value

? --- -----
? ...
? keys map[4:1549347108 5:1549347109 6:1549347110]
? latest_version 6
? min_available_version 0
? min_decryption_version 4
? min_encryption_version 0
Will Vault decrypt this data for you by running the following command?
? $ vault write transit/decrypt/prod-customer ciphertext="vault:v4:Xa1f9FIJtn13em/Wb7QCsXsU/kCOn7..."

A. Yes, because the minimum decryption key configuration is set to 4
B. No, since the latest version of the key is 6

Answer: A

NEW QUESTION 133
- (Topic 3)
True or False? A token can be renewed up until the max TTL, even if the TTL has been reached.

A. True
B. False

Answer: B

NEW QUESTION 137
- (Topic 3)
Based on the output below, how many policies have been added to Vault?
$ vault policy list base
default root
web-app-1 automation-team

A. 3
B. 4
C. 1
D. 2

Answer: A

NEW QUESTION 140
- (Topic 3)
In Vault, there are two main types of tokens, batch and service. Which of the following is true about the renewable capabilities of each?

A. Batch tokens cannot be renewed, but service can be renewed up to the max TTL
B. Tokens cannot be renewed without reauthenticating to Vault
C. Service tokens cannot be renewed, but batch can be renewed up to the max TTL
D. Both batch and service tokens can be renewed up to the max TTL

Answer: A

NEW QUESTION 145
- (Topic 3)
After setting up a new HashiCorp Vault server with the default configurations, which method can be used to unseal Vault?

A. Log on to each Vault node and provide the root token
B. Running vault operator init to regenerate unseal keys and automatically unseal the Vault
C. Submit a threshold of unseal keys to reconstruct the root key
D. Restart the Vault service, which will automatically unseal it

Answer: C

NEW QUESTION 149
- (Topic 3)
True or False? You can create and update Vault policies using the UI.

A. True
B. False

Answer: A

NEW QUESTION 152
- (Topic 3)
What command can be used to update a Vault policy named web-app-1 using the command line?

A. vault policy create web-app-1 web.hcl
B. vault policy fmt web.hcl
C. vault policy update web-app-1 web.hcl
D. vault policy write web-app-1 web.hcl

Answer: D

NEW QUESTION 154
- (Topic 3)
True or False? To encrypt existing encrypted data with the latest version of the encryption key, you need to first decrypt it and then request Vault to re-encrypt it with the latest version of the encryption key.

A. True
B. False

Answer: B

NEW QUESTION 156
- (Topic 3)
Jarrad is an AWS engineer and has provisioned a new EC2 instance running MySQL since his application requires a specific MySQL version. He wants to integrate Vault into his workflow but is new to Vault. What secrets engine should Jarrad use to integrate this new database running in AWS?

A. azure
B. database
C. kv
D. aws

Answer: B

NEW QUESTION 160
- (Topic 3)
Assuming default configurations, which of the following operations require a threshold of key shares to perform? (Select three)

A. Rotating the Vault encryption key to adhere to internal security policies
B. Unsealing Vault after a scheduled maintenance to install patches
C. Generating a new root token as a break-glass procedure
D. Creating a new set of recovery keys due to an employee leaving the organization

Answer: BCD

NEW QUESTION 161
- (Topic 3)
What command would you use to enable the Kubernetes secrets engine at the path of /k8s-cluster?

A. vault secrets enable -path=k8s-cluster kubernetes
B. vault kv put k8s-cluster type=kubernetes
C. vault write sys/mounts/k8s-cluster
D. vault secrets enable kubernetes -path=k8s-cluster

Answer: A

NEW QUESTION 165
- (Topic 3)
You need to create a limited-privileged token that isn??t impacted by the TTL of its parent. What type of token should you create?

A. Service token with a use limit
B. Orphan token
C. Periodic token
D. Root token

Answer: B

NEW QUESTION 166
- (Topic 3)
Short-lived, dynamically generated secrets provide organizations with many benefits. Select the benefits from the options below. (Select four)

A. Each application instance can generate its own credentials, rather than using a shared credential across all application instances
B. Credentials only exist when needed
C. Applications only have access to privileged accounts when needed
D. Credentials accidentally checked into a code repo or discovered in a text file are likely to be invalid
E. Dynamic credentials do not change, so legacy applications can easily take advantage of them

Answer: ABCD

NEW QUESTION 171
- (Topic 3)
Which of the following auth methods are intended for machine-to-machine authentication, and not necessarily human (operator) authentication? (Select four)

A. Okta
B. Tokens

C. TLS Certificates
D. Cloud-based Auth methods (AWS, Azure, GCP)
E. LDAP
F. AppRole

Answer: BCDF

NEW QUESTION 176
- (Topic 3)
Hanna is working with Vault and has been assigned a namespace called integration, where she stores all her secrets. Hanna configured her application to use the following API request, but the request is failing. What changes below will help Hanna correctly retrieve the secret? (Select two)
$ curl \
--header "X-Vault-Token:hvs.lzrmRe5Y3LMcDRmOttEjWoag" \
--request GET \ https://vault.example.com:8200/v1/secret/data/my-secret

A. $ curl --header "X-Vault-Token:hvs.lzrmRe5Y3LMcDRmOttEjWoag" --request GET\integration https://vault.example.com:8200/v1/secret/data/my-secret
B. $ curl --header "X-Vault-Token:hvs.lzrmRe5Y3LMcDRmOttEjWoag" --request GET -- namespace "integration" https://vault.example.com:8200/v1/secret/data/my-secret
C. $ curl --header "X-Vault-Token:hvs.lzrmRe5Y3LMcDRmOttEjWoag" --request GET https://vault.example.com:8200/v1/integration/secret/data/my-secret
D. $ curl --header "X-Vault-Token:hvs.lzrmRe5Y3LMcDRmOttEjWoag" --header "X-Vault- Namespace:integration" --request GET https://vault.example.com:8200/v1/secret/data/my- secret

Answer: CD

NEW QUESTION 178
- (Topic 3)
What is the default value of the VAULT_ADDR environment variable?

A. http://127.0.0.1:8200
B. https://vault.example.com:8200
C. https://127.0.0.1:8200
D. http://vault.example.com:8200

Answer: C

NEW QUESTION 181
- (Topic 3)
What is the default TTL for tokens in Vault if one is not specified?

A. 24 hours (1 day)
B. 15 minutes
C. 768 hours (32 days)
D. 60 minutes (1 hour)

Answer: C

NEW QUESTION 182
- (Topic 3)
What API endpoint is used to enable and configure a secrets engine?

A. /v1/sys/init
B. /v1/sys/mounts
C. /v1/sys/config
D. /v1/sys/plugins/catalog

Answer: B

NEW QUESTION 186
- (Topic 3)
Which of the following are supported auth methods for Vault? (Select six)

A. AWS
B. Kubernetes
C. Token
D. OIDC/JWT
E. Userpass
F. Cubbyhole
G. AppRole

Answer: ABCDEG

NEW QUESTION 188
- (Topic 3)
A DevOps engineer has set up LDAP and GitHub auth methods. The engineer must ensure user Sarah, who authenticates via either method, has consistent access permissions. Which approach correctly describes how to achieve this in Vault?

A. Create an entity for Sarah and map both her LDAP and GitHub identities as entity aliases to this single entity

B. Create an external group and add the LDAP and GitHub providers as members of the group
C. Create separate policies for each auth method and manually ensure they remain synchronized
D. Configure a trust relationship between the LDAP and GitHub providers to ensure Sarah??s account is synced

Answer: A

NEW QUESTION 189
- (Topic 3)
You need to decrypt customer data to provide it to an application. When you run the decryption command, you get the output below. Why does the response not directly reveal the cleartext data?
$ vault write transit/decrypt/phone_number ciphertext="vault:v1:tgx2vsxtlQRfyLSKvem..." Key Value
--- -----
plaintext aGFzaGljb3JwIGNlcnRpZmllZDogdmF1bHQgYXNzb2NpYXRl

A. The user does not have permission to view the cleartext data
B. The output is base64 encoded
C. The output is actually a response wrapped token that needs to be unwrapped
D. The original data must have been encrypted

Answer: B

NEW QUESTION 194
- (Topic 3)
Which of the following tokens are representative of a batch token? (Select two)

A. hvr.AAAAAQL_tyer_gNuQqvQYPVQgsNxjap_YW1NB2m4CDHHadQo7rF2XLFGdwNJplA ZNKbfloOvifrbpRCGdgG1taTqmC7Da_qftN64zeL10SmNwEoDTiPzC_1aS1KExbtVftU3Sx 16cBVqaynwsYRDfVnfTAffE
B. hvb.CAESIKOOSODDNGUJQe3EmsS8EQthulLjxRDhan_Axte2OrmPGiAKHGh2cy5KVnN hM25JdG82cDB0a1ZDbWhPTlAyekMQHg
C. hvb.AAAAAQJnAGuRT_z8FD_jOwP26zYaNzJ456_SVqse0oXtaqrpaLUC3LlHrUoJhQPylG X7A6K_dcS0shiql6g5-BVpz0QIkCm7ePFQVjDT2HcIf8C6FNgkW313vYgBGP8lzQHebtspC0pqK64cfyU_qPKIka2 u4ng-jsoy
D. hvs.493n55sZp2lX2zyQfpkHTkL4

Answer: BC

NEW QUESTION 198
- (Topic 3)
You are enabling a secrets engine in Vault using the CLI. What subcommands are available when using the vault secrets command? (Select five)

A. update
B. migrate
C. tune
D. enable
E. move
F. disable
G. list

Answer: CDEFG

NEW QUESTION 202
- (Topic 3)
Tanner manages a data processing application and needs to be sure the data being processed is encrypted so it is securely stored post-processing. Which secrets engines can encrypt data? (Select three)

A. transit
B. KMIP
C. SSH
D. transform

Answer: ABD

NEW QUESTION 206
- (Topic 3)
Vault operators can create two types of groups in Vault. What are the two types?

A. External groups
B. Security groups
C. Policy groups
D. Internal groups

Answer: AD

NEW QUESTION 207
- (Topic 3)
What features are offered by the Vault Agent? (Select three)

A. Auditing
B. Templating

C. Auto-auth
D. Secret caching

Answer: BCD

NEW QUESTION 211
- (Topic 3)
True or False? The following policy permits a user to read secrets contained in the path secrets/cloud/apps/jenkins?
text CollapseWrapCopy
path "secrets/cloud/apps/jenkins/*" {
capabilities = ["create", "read", "update", "delete", "list"]
}

A. True
B. False

Answer: B

NEW QUESTION 212
- (Topic 3)
When a lease is created, what actions can be performed by using only the lease ID? (Choose two)

A. Renew the lease
B. Revoke the lease
C. Extend the max TTL for the lease
D. Authenticate using the lease ID

Answer: AB

NEW QUESTION 215
- (Topic 3)
Which of the following are valid types of tokens available in Vault? (Select five)

A. Primary token
B. Batch token
C. Orphan service token
D. Service token
E. Root token
F. Periodic service token

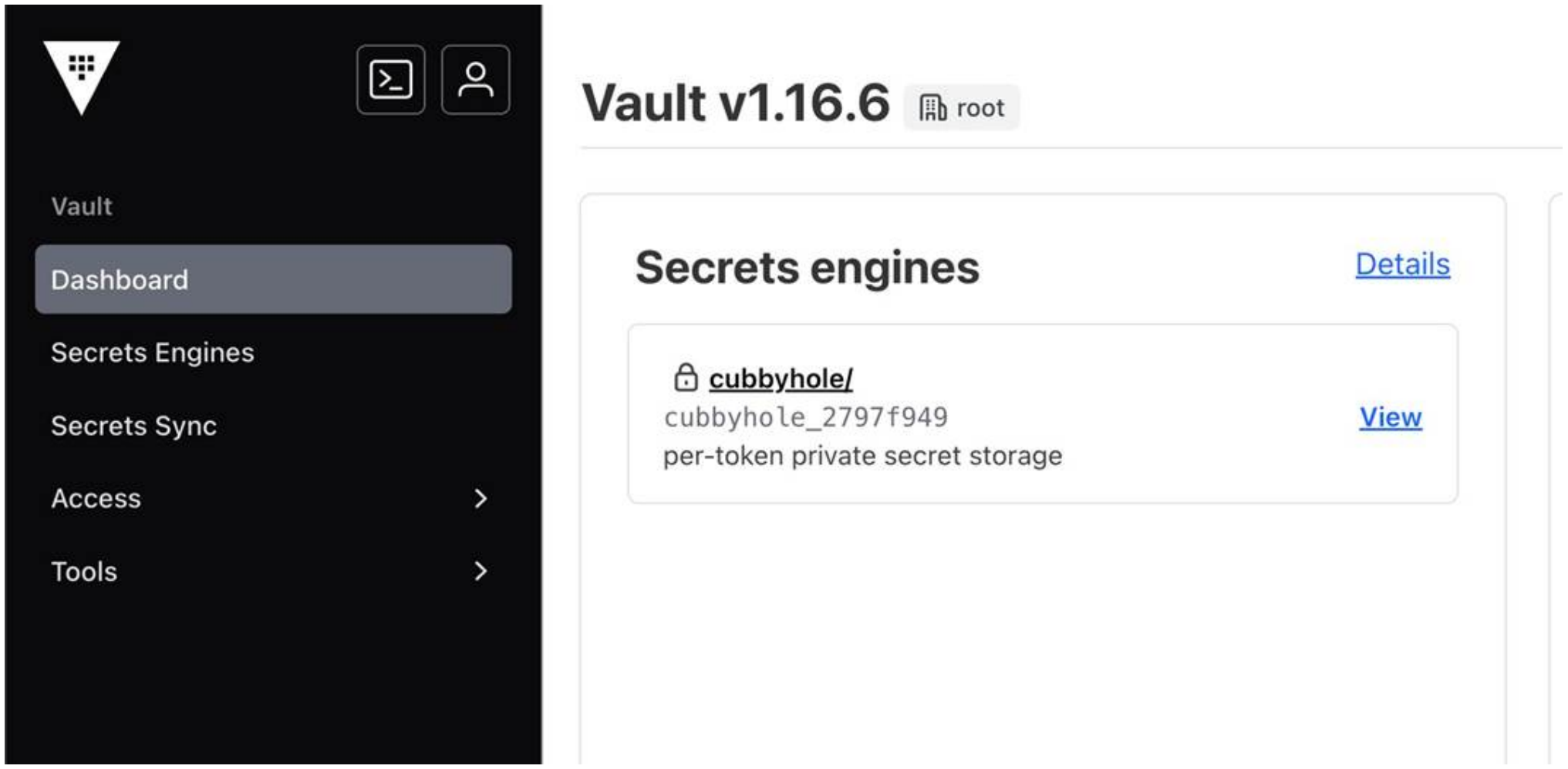
Answer: BCDEF

NEW QUESTION 217
- (Topic 4)
A new application is being provisioned in your environment. The application requires the generation of dynamic credentials against the Oracle database in order to read reporting data. Which is the best auth method to use to permit the application to authenticate to Vault?

A. OIDC
B. GitHub
C. Userpass
D. AppRole

Answer: D

NEW QUESTION 218
- (Topic 4)
A developer has requested access to manage secrets at the path kv/apps/webapp01. You create the policy below which gives them the proper access:
path "kv/apps/webapp01" {
capabilities = ["read", "create", "update", "list"]
}
However, when the developer logs in to the Vault UI, they see the following screenshot and cannot access the desired secret. Why can??t the developer see the secrets they need?



A. The Vault UI isn??t enabled for the developer, therefore they will only see the default options
B. The key/value secrets engine isn??t available in the Vault UI, therefore the developer should use a different Vault interface instead
C. The policy doesn??t permit list access to the paths prior to the secret so the Vault UI doesn??t display the mount path
D. The secrets are stored under the cubbyhole secrets engine, so the developer should browse to that secrets engine

Answer: C

NEW QUESTION 220
- (Topic 4)
Frapps, Inc. is a coffee startup specializing in frozen caffeinated beverages. Their new customer loyalty web app uses Vault to store sensitive information, choosing Integrated Storage for its benefits. Select the benefits the organization would see by using Integrated Storage over other storage backends (Select four)

A. Eliminates network communication between hosts, requiring no open ports between hosts
B. Uses the SERF gossip protocol to enable communication between cluster nodes
C. Eliminates the requirement to deploy and manage a separate platform for storing encrypted data
D. Simplified troubleshooting since Integrated Storage is a built-in solution
E. Reduces operational overhead since all configuration is within Vault itself
F. Immediate access to storage since the data is stored locally on disk

Answer: CDEF

NEW QUESTION 222
- (Topic 4)
Over a few years, you have a lot of data that has been encrypted by older versions of a Transit encryption key. Due to compliance regulations, you have to re-encrypt the data using the newest version of the encryption key. What is the easiest way to complete this task without putting the data at risk?

A. Rotate the encryption key used to encrypt the data
B. Decrypt the data manually and encrypt it with the latest version
C. Use the transit rewrap feature
D. Create a new master key used by Vault

Answer: C

NEW QUESTION 226
- (Topic 4)
Why are short-lived, dynamic secrets in Vault more secure than long-lived, static credentials?

A. They provide better performance by caching credentials for longer durations
B. They are created on-demand and expire after a short period, minimizing the risk of credential leakage
C. They eliminate the need for authentication, allowing seamless access to Vault-managed systems
D. They automatically rotate on a set schedule, reducing the need for manual intervention

Answer: B

NEW QUESTION 231
- (Topic 4)
Your organization recently suffered a security breach on a specific application, and the security response team believes that MySQL database credentials were likely obtained during the event. The application generated the credentials using the database secrets engine in Vault mounted at the path database/. How can you

quickly revoke all of the secrets generated by this secrets engine?

A. vault token revoke database/*
B. vault secrets disable mysql
C. vault lease renew database/creds/mysql
D. vault lease revoke -prefix database/

Answer: D

NEW QUESTION 232
- (Topic 4)
Which of the following are considered benefits of using policies in Vault? (Select three)

A. Policies are assigned to a token on a 1:1 basis to eliminate conflicting policies
B. Provides granular access control to paths within Vault
C. Policies have an implicit deny, meaning that policies are deny by default
D. Policies provide Vault operators with role-based access control

Answer: BCD

NEW QUESTION 236
- (Topic 4)
A large organization uses Vault for various use cases with multiple auth methods enabled. A user can authenticate via LDAP, OIDC, or a local userpass account, but they receive different policies for each method and often need to log out and back in for different actions. What can be configured in Vault to ensure users have consistent policies regardless of their authentication method?

A. Enable the SSH secrets engine and instruct the user to obtain credentials using the new secrets engine
B. Create a new entity and map the aliases from each of the available auth methods
C. Assign the default policy to the user's policy used by each auth method
D. Provide the user with an AppRole role-id and secret-id for authentication

Answer: B

NEW QUESTION 239
- (Topic 4)
Your team uses the Transit secrets engine to encrypt all data before writing it to a MySQL database server. During testing, you manually retrieve ciphertext from the database and decrypt it to ensure the data can be read. After decrypting the data, you are worried something is wrong because the plaintext data isn??t legible. Why can you not read the original plaintext data after decrypting the ciphertext?
? $ vault write transit/decrypt/krausen-key ciphertext=vault:v1:8SDd3WHDOjf7mq69C.....
? Key Value
? --- -----
? plaintext Zml2ZSBzdGFyIHByYWN0aWNlIGV4YW1zIGJ5IGJyeWFuIGtyYXVzZW4=

A. The incorrect key was selected when decrypting the ciphertex
B. Use the correct key to successfully read the data
C. The incorrect key version was used to decrypt the dat
D. Update the ciphertext and change the v1 to v3 to use the latest key version
E. The plaintext is Base64 encode
F. Decode the plaintext to see the original data
G. The data was also encrypted on the databas
H. Therefore Vault cannot decrypt the original data

Answer: C

NEW QUESTION 240
- (Topic 4)
There are a few ways in Vault that can be used to obtain a root token. Select the valid methods from the answers below. (Select three)

A. Generating a root token using a quorum of recovery keys when using Vault auto unseal
B. Initializing Vault when first creating the cluster by using vault operator init
C. Using a batch DR operation token to create a new root token in the event of an emergency
D. Running the command vault token create when using a valid root token

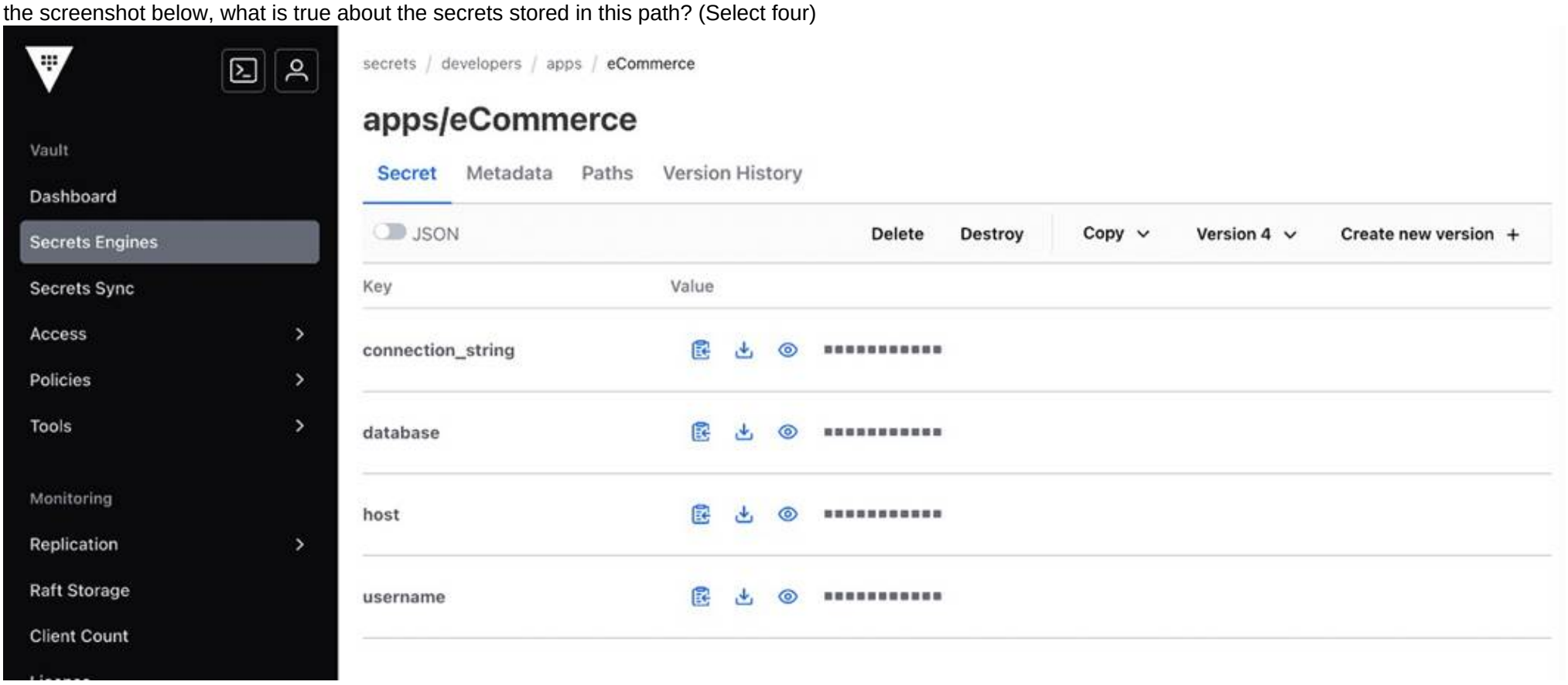
Answer: ABD

NEW QUESTION 241
- (Topic 4)
You have a CI/CD pipeline using Terraform to provision AWS resources with static privileged credentials. Your security team requests that you use Vault to limit AWS access when needed. How can you enhance this process and increase pipeline security?

A. Enable the SSH secrets engine and have Terraform generate dynamic credentials when deploying resources in AWS
B. Enable the Transit secrets engine to encrypt the AWS credentials and have Terraform retrieve these credentials when needed
C. Store the AWS credentials in the Vault KV store and use the Vault provider to obtain these credentials on each terraform apply
D. Enable the aws secrets engine and configure Terraform to dynamically generate a short- lived AWS credential on each terraform apply

Answer: D

NEW QUESTION 244
- (Topic 4)
You are working on a new project and need to retrieve a secret from Vault. You log into the Vault UI and browse to the path where the secret is stored. Based on the screenshot below, what is true about the secrets stored in this path? (Select four)



A. The secrets are stored in a KV v1 secrets engine
B. The user does not have permission to delete the secret
C. The secrets are stored in a KV v2 secrets engine
D. The secrets engine is mounted at the path developers/
E. There are four previous versions of the secret
F. The user has additional permissions on the path beyond just list and read

Answer: CDEF

NEW QUESTION 246
- (Topic 4)
Vault is configured with the oidc auth method and you need to log in using the CLI. What command would you use to authenticate so you can make configuration changes to Vault?

A. vault login -method=oidc username=bryan
B. vault auth oidc
C. vault login auth/oidc/users/bryan
D. vault login username=bryan

Answer: A

NEW QUESTION 249
- (Topic 4)
You need to write a new policy for Vault for a group of users on the automation team. The requirements stipulate that each user (and all future users) get access to their own private section of a KV secrets engine at the path kv/team/ and be able to manage their own secrets. Which policy below meets these requirements while minimizing the administrative effort and following the principle of least privilege?

A. path "secret/data/groups/{{identity.groups.ids.2f62-9503-42aa7A869741.name}}/" { capabilities = ["list"] }
B. path "kv/team/frank/" { capabilities = ["create", "update", "read", "delete"] } path "kv/team/steve/" { capabilities = ["create", "update", "read", "delete"] } path "kv/team/bryan/ " { capabilities = ["create", "update", "read", "delete"] }
C. path "kv/team/" { capabilities = ["create", "update", "read", "delete"] }
D. path "kv/team/{{identity.entity.id}}/" { capabilities = ["create", "update", "read", "delete"] } path "kv/team/{{identity.entity.id}}" { capabilities = ["create", "update", "read", "delete"] }

Answer: D

NEW QUESTION 250
- (Topic 4)
True or False? After rotating a transit encryption key, all data encrypted with the previous version must be rewrapped or re-encrypted with the new key.

A. True
B. False

Answer: B

NEW QUESTION 252
- (Topic 4)
You are planning the deployment of your first Vault cluster and have decided to use Integrated Storage as the storage backend. Where do you configure the

storage backend to be used by Vault?

A. In the systemd service file
B. Inside the Vault service once Vault is up and running
C. In the Vault configuration file
D. In the Vault Agent sink file

Answer: C

NEW QUESTION 253
- (Topic 4)
Your organization audited an essential application and found it isn??t securely storing data. For added security, auditors recommended encrypting all data before storing it in a backend database, and the application server should not store encryption keys locally. Which secrets engine meets these requirements?

A. PKI secrets engine
B. SSH secrets engine
C. Transit secrets engine
D. Cubbyhole secrets engine

Answer: C

NEW QUESTION 255
- (Topic 4)
Which of the following is true about the token authentication method in Vault? (Select three)

A. The token auth method is automatically enabled in Vault and cannot be disabled
B. External authentication mechanisms, such as GitHub, are used to dynamically create tokens
C. The token auth method is used as the first method of authentication for Vault for a newly initialized Vault node/cluster
D. Tokens cannot be used directly; they must be used in conjunction with one of Vault??s many auth methods

Answer: ABC

NEW QUESTION 258
- (Topic 4)
You are using Vault to generate dynamic credentials for a Microsoft SQL server to perform queries for a month-end report. The report seems to be taking much longer than expected due to degradation on the underlying server, and you are afraid that Vault might automatically revoke the credentials. How can you extend the time the credentials are valid to ensure your month-end query is successful?

A. Renew the lease
B. Generate a new lease
C. Create a new role within the secrets engine for the database
D. Revoke the lease

Answer: A

NEW QUESTION 260
- (Topic 4)
All Vault instances, or clusters, include two built-in policies that are created automatically. Choose the two policies below and the correct information regarding each policy. (Select two)

A. The root policy is created automaticall
B. This policy provides superuser privileges and cannot be deleted
C. The admin policy is created automaticall
D. It provides administrative permissions but can be deleted if needed
E. The default policy is created automaticall
F. This policy can be modified but not deleted
G. The default policy is created automaticall
H. This policy cannot be modified but it can be deleted

Answer: AC

NEW QUESTION 263
- (Topic 4)
You have a new team member on the Vault operations team. Their first task is to rotate the encryption key in Vault as part of the organization??s security policy. However, when they log in, they get an access denied error when attempting to rotate the key. The policy being used is below. Why can??t the user rotate the encryption key?
path "auth/*" {
capabilities = ["create", "read", "update", "delete", "list"]
}
path "sys/rotate" {
capabilities = ["read", "update"]
}

A. The policy requires sudo privileges since it is a root-protected path
B. The policy doesn??t include create privileges so a new encryption key can??t be created
C. The policy should include sys/rotate/<name of key> as part of the path
D. The encryption key has a minimum TTL, therefore the key cannot be rotated until that time expires

Answer: A

NEW QUESTION 268
- (Topic 4)
To secure your applications, your organization uses certificates generated by a public CA. However, this strategy has proven expensive and you have to revoke certificates even though they have additional time left. What Vault plugin can be used to quickly generate

A. X.509 certificates to secure your internal applications?
B. Identity secrets engine
C. PKI secrets engine
D. SSH secrets engine
E. Transit secrets engine

Answer: B

NEW QUESTION 272
- (Topic 4)
Which of the following capabilities can be used when writing a Vault policy? (Select four)

A. list
B. deny
C. apply
D. root
E. create
F. write

Answer: ABEF

NEW QUESTION 277
- (Topic 4)
Which core component of Vault can store, generate, or encrypt data for organizations?

A. auth method
B. storage backend
C. secrets engine
D. audit device

Answer: C

NEW QUESTION 279
- (Topic 4)
An Active Directory admin created a service account for an internal application. You want to store these credentials in Vault, allowing a CI/CD pipeline to read and configure the application with them during provisioning. Vault should maintain the last 3 versions of this secret. Which Vault secrets engine should you use?

A. The KV secrets engine
B. The LDAP secrets engine
C. The Identity secrets engine
D. The KV v2 secrets engine

Answer: D

NEW QUESTION 282
- (Topic 4)
Your organization runs workloads on both AWS and Azure for production applications. The security team has requested that a single Vault authentication mechanism be enabled to support applications on both public cloud platforms. Which of the following would be a valid auth method you can use?

A. AWS
B. GitHub
C. AppRole
D. Azure

Answer: C

NEW QUESTION 285
- (Topic 4)
You are using Vault CLI and enable the database secrets engine on the default path of database/. However, the DevOps team wants to enable another database secrets engine for testing but receives an error stating the path is already in use. How can you enable a second database secrets engine using the CLI?

A. vault secrets enable database database2/
B. vault secrets enable -force database
C. vault secrets enable -path=database2 database
D. vault secrets enable database2/

Answer: C

NEW QUESTION 290

- (Topic 4)
You have multiple Vault clusters in your environment, one for test and one for production. You have the CLI installed on your local machine and need to target the production cluster to make configuration changes. What environment variable can you set to target the production cluster?

A. VAULT_REDIRECT_ADDR
B. VAULT_CLUSTER_ADDR
C. VAULT_ADDR
D. VAULT_CAPATH

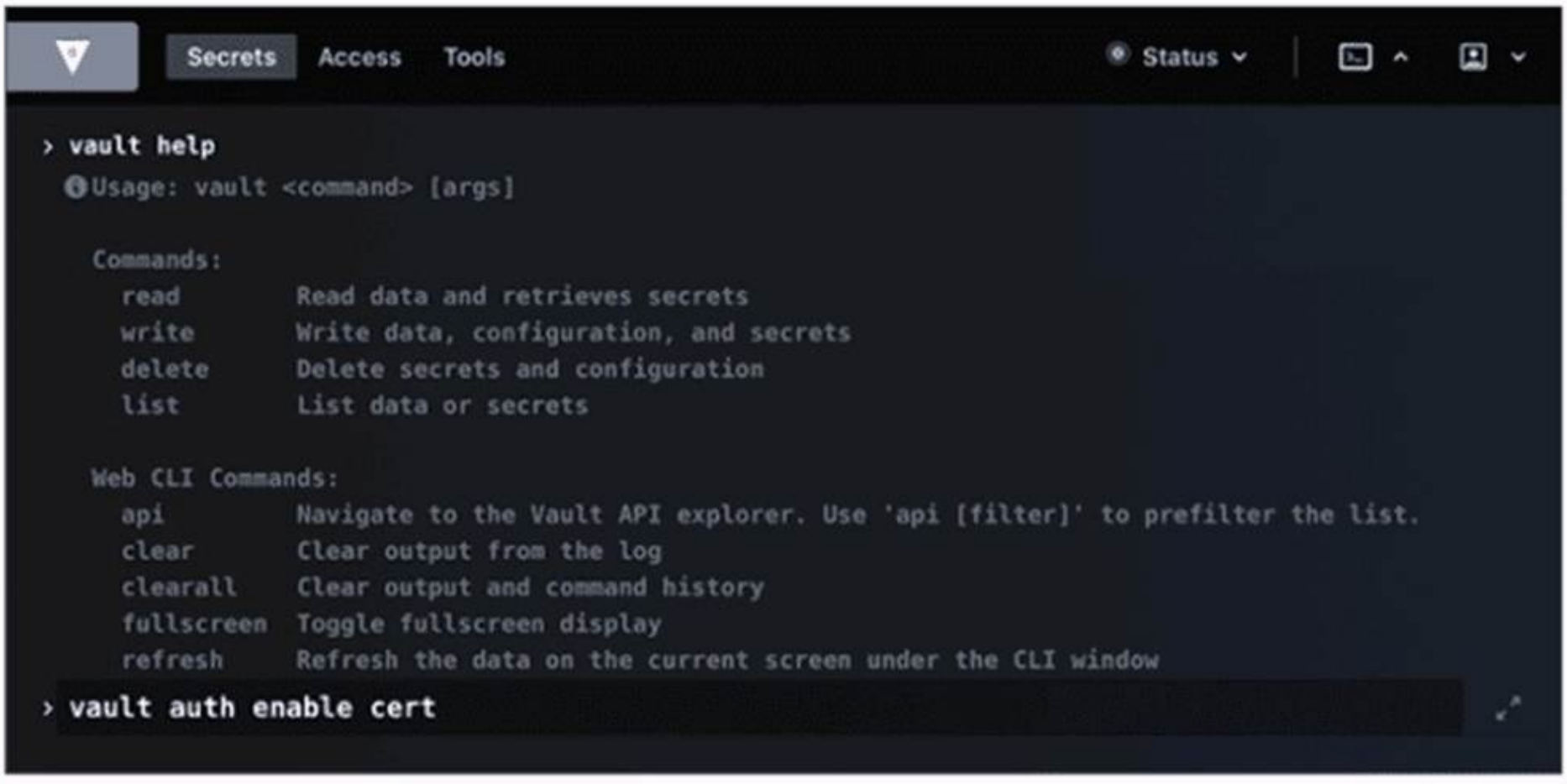
Answer: C

NEW QUESTION 295
- (Topic 5)
Which of the following statements are true about Vault policies? Choose two correct answers.

A. The default policy can not be modified
B. You must use YAML to define policies
C. Policies provide a declarative way to grant or forbid access to certain paths and operations in Vault
D. Vault must be restarted in order for a policy change to take an effect
E. Policies deny by default (empty policy grants no permission)

Answer: CE

NEW QUESTION 300
- (Topic 5)
Running the second command in the GUI CLI will succeed.



A. True
B. False

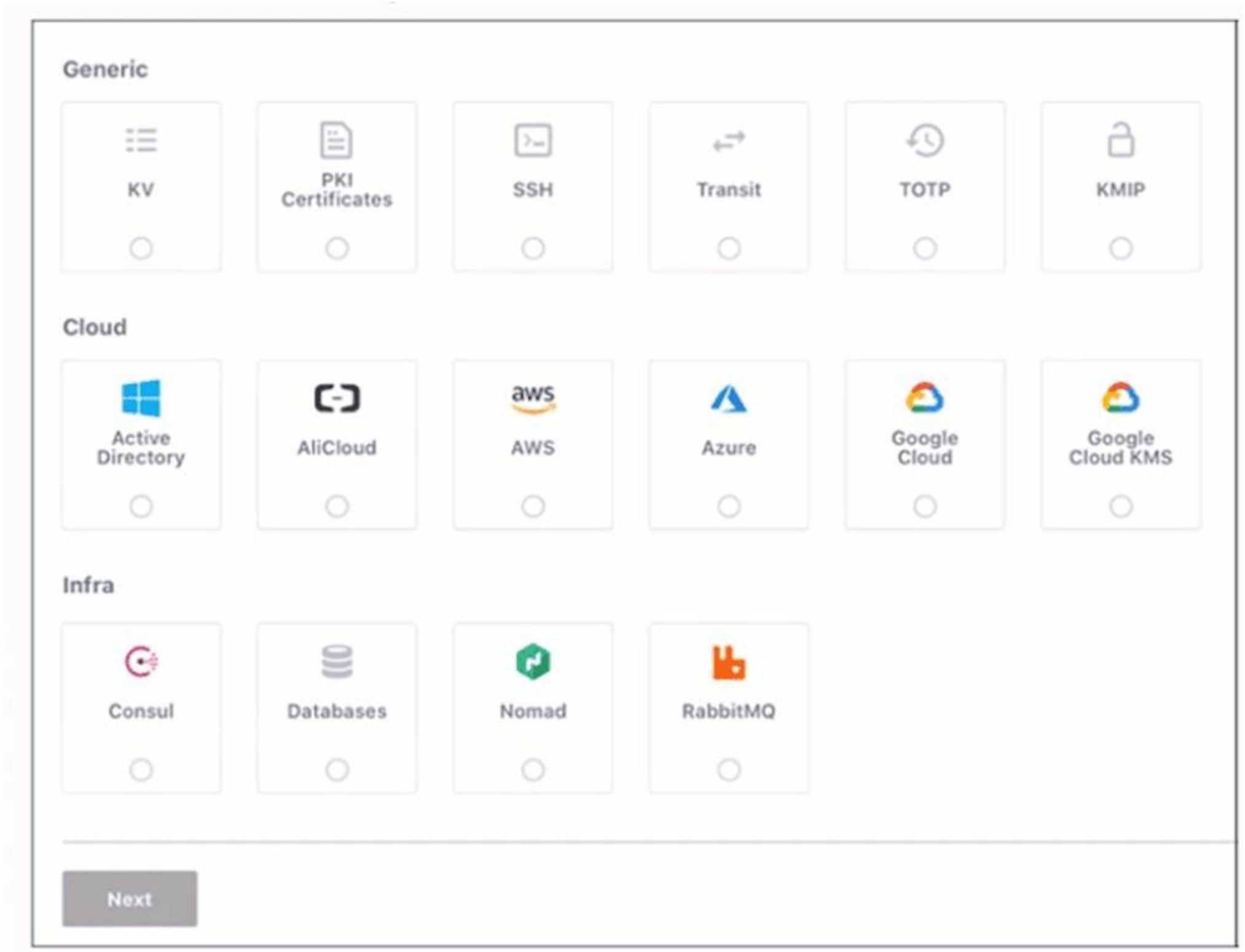
Answer: B

NEW QUESTION 304
- (Topic 5)
An organization would like to use a scheduler to track & revoke access granted to a job (by Vault) at completion. What auth-associated Vault object should be tracked to enable this behavior?

A. Token accessor
B. Token ID
C. Lease ID
D. Authentication method

Answer: C

NEW QUESTION 305
- (Topic 5)
Use this screenshot to answer the question below:



When are you shown these options in the GUI?

A. Enabling policies
B. Enabling authentication engines
C. Enabling secret engines
D. Enabling authentication methods

Answer: D

NEW QUESTION 306
- (Topic 5)
Vault supports which type of configuration for source limited token?

A. Cloud-bound tokens
B. Domain-bound tokens
C. CIDR-bound tokens
D. Certificate-bound tokens

Answer: C

NEW QUESTION 310
- (Topic 5)
What are orphan tokens?

A. Orphan tokens are tokens with a use limit so you can set the number of uses when you createthem
B. Orphan tokens are not children of their parent; therefore, orphan tokens do not expire when their parent does
C. Orphan tokens are tokens with no policies attached
D. Orphan tokens do not expire when their own max TTL is reached

Answer: D

NEW QUESTION 314
- (Topic 5)
Which of the following describes usage of an identity group?

A. Limit the policies that would otherwise apply to an entity in the group
B. When they want to revoke the credentials for a whole set of entities simultaneously
C. Audit token usage
D. Consistently apply the same set of policies to a collection of entities

Answer: D

NEW QUESTION 318
- (Topic 5)
Where does the Vault Agent store its cache?

A. In a file encrypted using the Vault transit secret engine
B. In the Vault key/value store
C. In an unencrypted file
D. In memory

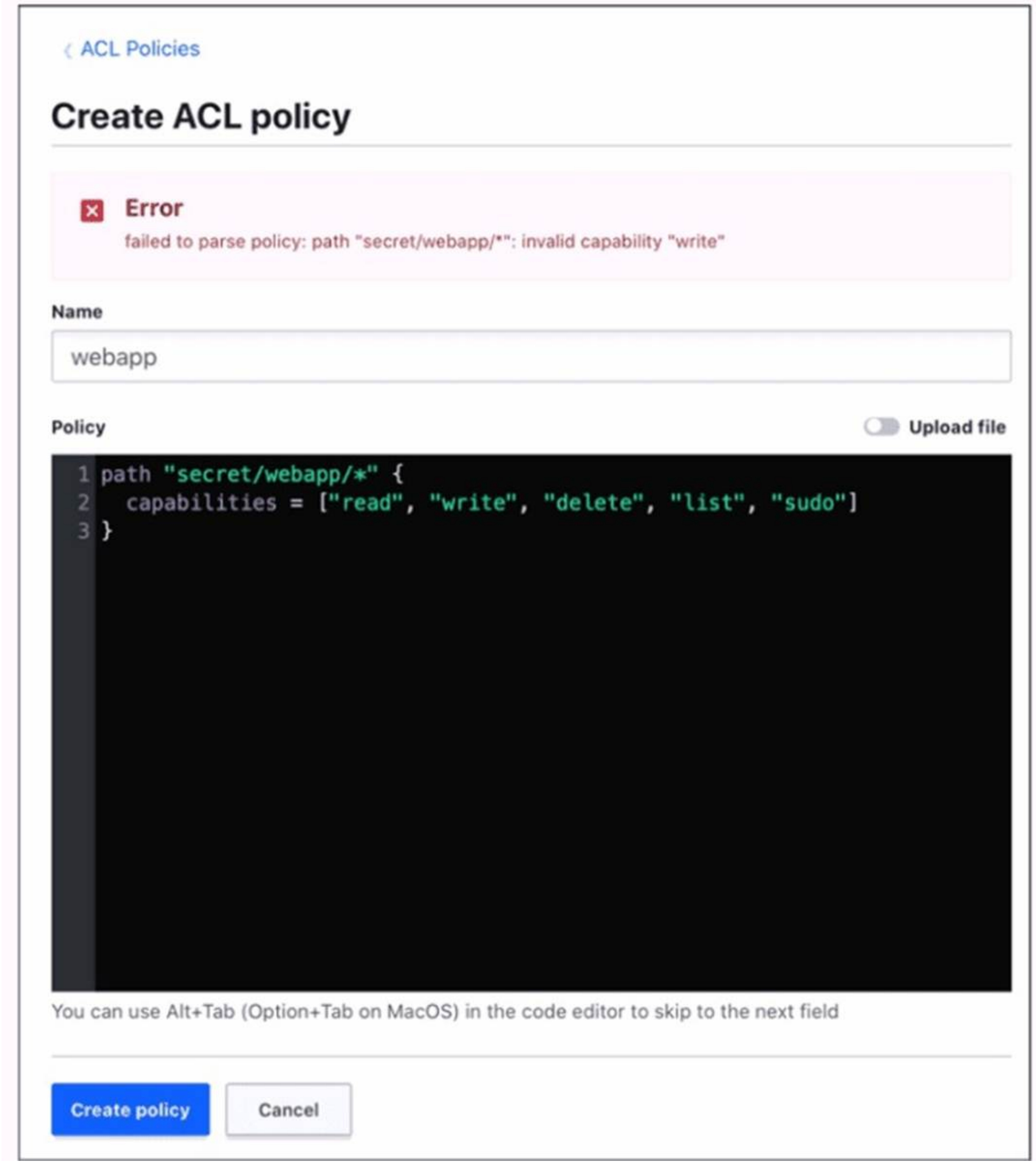
Answer: D

NEW QUESTION 320
- (Topic 5)
Which of the following vault lease operations uses a lease _ id as an argument? Choose two correct answers.

A. renew
B. revoke -prefix
C. create
D. describe
E. revoke

Answer: AE

NEW QUESTION 321
- (Topic 5)
When creating a policy, an error was thrown:



Which statement describes the fix for this issue?

A. Replace write with create in the capabilities list
B. You cannot have a wildcard (" • ") in the path
C. sudo is not a capability

Answer: A

NEW QUESTION 325
- (Topic 5)
When unsealing Vault, each Shamir unseal key should be entered:

A. Sequentially from one system that all of the administrators are in front of
B. By different administrators each connecting from different computers
C. While encrypted with each administrators PGP key
D. At the command line in one single command

Answer: B

NEW QUESTION 327
- (Topic 5)
Which of the following statements describe the CLI command below? S vault login -method-1dap username-mitche11h

A. Generates a token which is response wrapped
B. You will be prompted to enter the password
C. By default the generated token is valid for 24 hours
D. Fails because the password is not provided

Answer: A

NEW QUESTION 329
- (Topic 5)
What is the Vault CLI command to query information about the token the client is currently using?

A. vault lookup token
B. vault token lookup
C. vault lookup self
D. vault self-lookup

Answer: B

NEW QUESTION 333
- (Topic 5)
What command creates a secret with the key "my-password" and the value "53cr3t" at path "my-secrets" within the KV secrets engine mounted at "secret"?

A. vault kv put secret/my-secrets/my-password 53cr3t
B. vault kv write secret/my-secrets/my-password 53cr3t
C. vault kv write 53cr3t my-secrets/my-password
D. vault kv put secret/my-secrets »y-password-53cr3t

Answer: A

NEW QUESTION 335
- (Topic 5)
Examine the command below.Output has been trimmed.

```
  $ vault write auth/approle/login \
    role_id="debb8f13-79ea-3e3d-8100-10711d85c1fb" \
    secret_id="31d52faa-5b0b-711d-2ea2-c197cff6081b"Key Value
---                   -----
token                 b.AAAAAQIlWH-DExezQvz-ZGWMhzsy8uWXEoQYHH6O...trimmed...
token_accessor        n/a
token_duration        1m
token_renewable       false
token_policies        ["shipping"]
identity_policies     []
policies              ["shipping"]
token_meta_role_name  shipping
```

Which of the following statements describe the command and its output?

A. Missing a default token policy
B. Generated token's TTL is 60 hours
C. Generated token is an orphan token which can be renewed indefinitely
D. Configures the AppRole auth method with user specified role ID and secret ID

Answer: BC

NEW QUESTION 339
- (Topic 5)
You have a 2GB Base64 binary large object (blob) that needs to be encrypted. Which of the following best describes the transit secrets engine?

A. A data key encrypts the blob locally, and the same key decrypts the blob locally.
B. To process such a large blo
C. Vault will temporarily store it in the storage backend.
D. Vault will store the blob permanentl
E. Be sure to run Vault on a compute optimized machine
F. The transit engine is not a good solution for binaries of this size.

Answer: D

NEW QUESTION 341
- (Topic 5)
A user issues the following cURL command to encrypt data using the transit engine and the Vault AP:

```
curl \
--header "X-Vault-Token: c4f280f6-fdb2-18eb-89d3-589e2e834cdb" \
--request POST \<
--data @payload.json \
http://127.0.0.1:8200/v1/transit/encrypt/my-key
```

Which payload.json file has the correct contents?

A.
```
{
  "plaintext": "dGhlIHF1aWNrIGJyb3duIGZveA=="
}
```

B.
```
{
  "ciphertext": "vault:v1:abcdefgh"
}
```

C.
```
{
  "data": {
    "plaintext": "dGhlIHF1aWNrIGJyb3duIGZveA=="
  }
}
```

D.
```
{
  "data": {
    "ciphertext": "vault:v1:abcdefgh"
  }
}
```

Answer: C

NEW QUESTION 346
- (Topic 5)
An authentication method should be selected for a use case based on:

A. The auth method that best establishes the identity of the client
B. The cloud provider for which the client is located on
C. The strongest available cryptographic hash for the use case
D. Compatibility with the secret engine which is to be used

Answer: A

NEW QUESTION 347
- (Topic 5)
Which of the following describes the Vault's auth method component?

A. It verifies a client against an internal or external system, and generates a token with the appropriate policies attached
B. It verifies a client against an internal or external system, and generates a token with root policy
C. It is responsible for durable storage of client tokens
D. It dynamically generates a unique set of secrets with appropriate permissions attached

Answer: A

NEW QUESTION 348
- (Topic 5)
An organization wants to authenticate an AWS EC2 virtual machine with Vault to access a dynamic database secret. The only authentication method which they can use in this case is AWS.

A. True
B. False

Answer: B

NEW QUESTION 352
- (Topic 5)
Which statement describes the results of this command: $ vault secrets enable transit

A. Enables the transit secrets engine at transit path
B. Requires a root token to execute the command successfully
C. Enables the transit secrets engine at secret path
D. Fails due to missing -path parameter
E. Fails because the transit secrets engine is enabled by default

Answer: A

NEW QUESTION 356
- (Topic 5)
Your DevOps team would like to provision VMs in GCP via a CICD pipeline. They would like to integrate Vault to protect the credentials used by the tool. Which secrets engine would you recommend?

A. Google Cloud Secrets Engine
B. Identity secrets engine
C. Key/Value secrets engine version 2
D. SSH secrets engine

Answer: A

NEW QUESTION 361
- (Topic 5)
When an auth method is disabled all users authenticated via that method lose access.

A. True
B. False

Answer: A

NEW QUESTION 362
- (Topic 5)
A web application uses Vault's transit secrets engine to encrypt data in-transit. If an attacker intercepts the data in transit which of the following statements are true? Choose two correct answers.

A. You can rotate the encryption key so that the attacker won??t be able to decrypt the data
B. The keys can be rotated and min_decryption_version moved forward to ensure this data cannot be decrypted
C. The Vault administrator would need to seal the Vault server immediately
D. Even if the attacker was able to access the raw data, they would only have encrypted bits (TLS in transit)

Answer: BD

NEW QUESTION 366
- (Topic 5)
How many Shamir's key shares are required to unseal a Vault instance?

A. All key shares
B. A quorum of key shares
C. One or more keys
D. The threshold number of key shares

Answer:

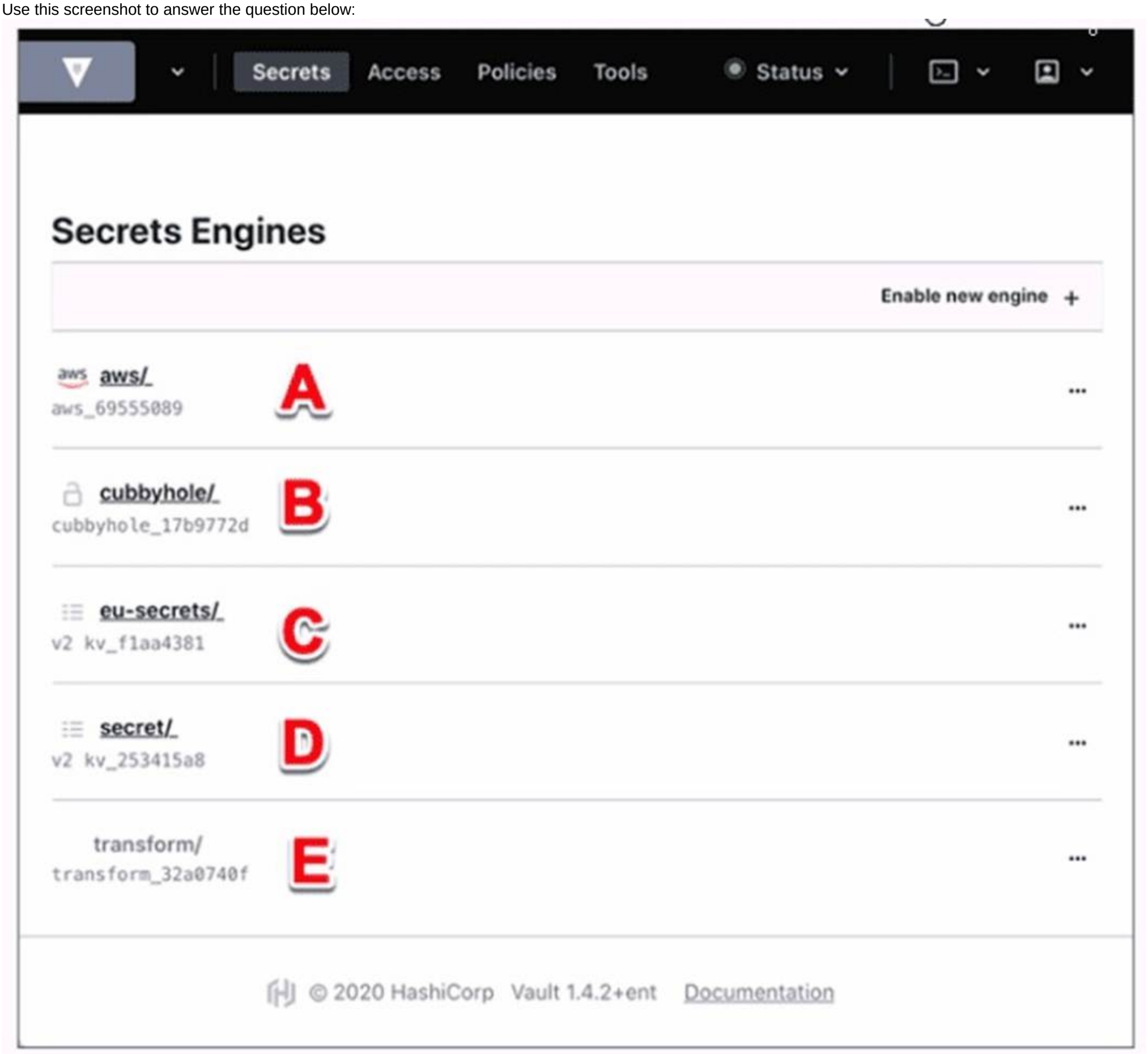
D

NEW QUESTION 368
- (Topic 5)
Which of the following statements describe the secrets engine in Vault? Choose three correct answers.

A. Some secrets engines simply store and read data
B. Once enabled, you cannot disable the secrets engine
C. You can build your own custom secrets engine
D. Each secrets engine is isolated to its path
E. A secrets engine cannot be enabled at multiple paths

Answer: ACD

NEW QUESTION 372
- (Topic 5)
Use this screenshot to answer the question below:



Where on this page would you click to view a secret located at secret/my-secret?

A. A
B. B
C. C
D. D
E. E

Answer: C

NEW QUESTION 373
- (Topic 5)
As a best practice, the root token should be stored in which of the following ways?

A. Should be revoked and never stored after initial setup
B. Should be stored in configuration automation tooling
C. Should be stored in another password safe
D. Should be stored in Vault

Answer: A

NEW QUESTION 376
.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

HCVA0-003 Practice Exam Features:

* HCVA0-003 Questions and Answers Updated Frequently

* HCVA0-003 Practice Questions Verified by Expert Senior Certified Staff

* HCVA0-003 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* HCVA0-003 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year